ОБНОВЛЕНО 16 МАР

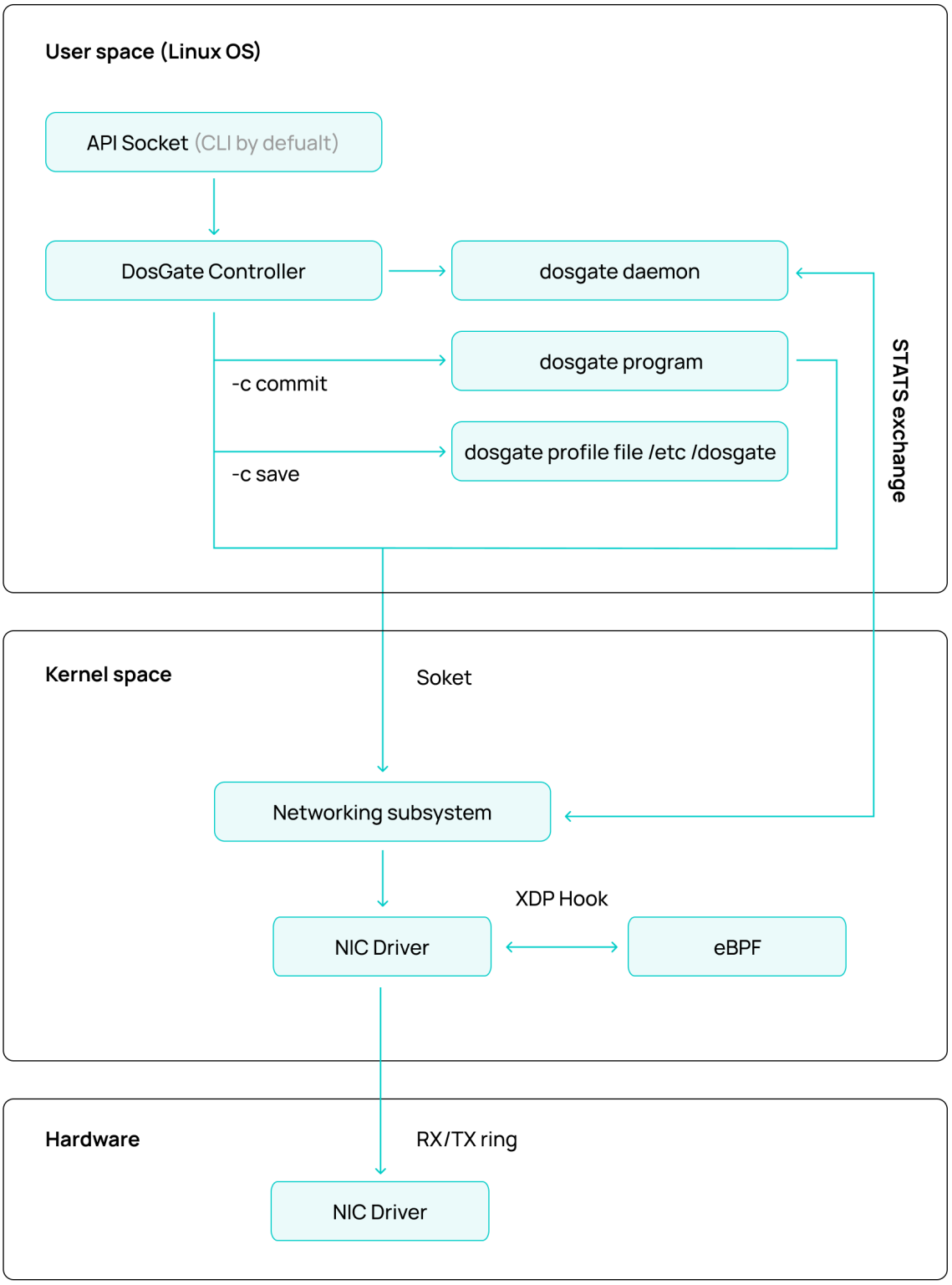
Компоненты платформы ПО

Архитектура платформы базируется на операционной системе Linux и включает в себя следующие ключевые компоненты:

DosGate Controller — программный модуль, предназначенный для трансляции пользовательских правил в машинный код, который впоследствии используется другими компонентами системы.

DosGate — ядро программы, содержащее скомпилированный машинный код, которое интегрируется в ядро Linux (Linux Kernel) посредством управления со стороны DosGate Controller.

DosGate Daemon — системный сервис, обеспечивающий сбор статистических данных и выполнение автоматического контроля. Этот компонент взаимодействует с ядром Linux, где выполняется загруженная программа DosGate.



Модули системы

DosGate содержит функционал, реализованный в виде модулей, распределённых по различным компонентам платформы:

Арена — набор сетевых интерфейсов, и применяемых к ним настроек.

Routing Program — программа, определяющая, в какой профиль должен быть направлен пакет на основании адреса назначения.

Профиль — набор правил, которые применяются к пакету, проходящему через профиль.

Пример взаимодействия модулей при обработке IP-пакета

Когда IP-пакет поступает на Сетевой интерфейс 1, система выполняет следующие шаги:

Идентификация Арены

Конфигурационный файл dosgate.conf используется для определения, к какой Арене относится данный сетевой интерфейс. После идентификации IP-пакет передается в программу маршрутизации (Routing Program) соответствующей Арены (например, Арена 1).

> **Примечание**
> DosGate Daemon использует конфигурационный файл dosgate.conf для сбора статистики. Собранные данные передаются в collectd, который обрабатывает и перенаправляет их в Graphite для последующего визуального отображения метрик.

Определение профиля защиты

На основании адреса назначения, указанного в Routing Program, выбирается профиль защиты, который должен быть применен к сетевому пакету.

Применение правил профиля защиты

Выбранный профиль защиты содержит наборы правил фильтрации и обработки пакетов. К поступившему сетевому пакету последовательно применяются эти правила.

Результат обработки пакета

После обработки согласно заданным правилам возможны три варианта действий:

1. Отбрасывание пакета (Drop): сетевой пакет считается нежелательным и удаляется.
2. Маршрутизация пакета (Route): сетевой пакет передается далее по назначению в соответствии с таблицей маршрутизации.
3. Возврат пакета (Reply): сетевой пакет передается в предыдущий этап обработки или возвращается в систему для дальнейшей обработки.

Такой подход позволяет гибко управлять сетевым трафиком и применять фильтрацию на основе правил, определённых для конкретных профилей защиты.